INFORMATION SECURITY

1 INTRODUCTION

1.1 Overview. These procedures establish site-specific requirements for the protection and control of DOE classified matter for Los Alamos National Laboratory (LANL) employees and its contractors.

1.2 Office of Institutional Coordination (OIC). The S-6 Information Security Team, 5-1802/MS G733, is responsible for establishing, coordinating, and supporting the implementation of these procedures.

1.3 Point of Contact (POC). S-2 is responsible for managing the institutional requirements of this document and any changes hereto.

1.4 Effective Date. These procedures are effective upon issue.

1.5 Cancellations. These procedures replace the previous LANL *Safeguards and Security Manual,* Chapter 9.

1.6 Table of Contents

2 Purpose.

To provide standardized procedures for the protection and control of classified matter within the Los Alamos National Laboratory complex.

3 Scope.

All LANL employees and its contractors who access classified matter are required to comply with these procedures. S-6 provides subject matter experts in all the areas covered by this section. Questions may be directed to information security experts at 665-1802.

4 Definitions

Outside Facility:	Outside the LANL complex
Within Facility:	LANL-wide complex (to include LAAO)

5 Precautions and Limitations.

All conceivable situations cannot be covered by these procedures; therefore, contact S-6 at 665-1802 for guidance regarding exceptions or circumstances not described herein.

6 Duties and Responsibilities

6.1 S-6 Information Security Team

6.1.1 Develops and issues formal procedures for the site-wide handling of classified matter.

6.1.2 Conducts Classified Matter Protection and Control (CMPC) Tier II self-assessments.

6.1.3 Ensures that procedures outlined in appropriate DOE directives and these procedures are being followed by organizations and individuals involved in the handling of classified matter.

6.1.4 Oversees the site training curriculum of document and part primary and alternate custodians.

6.1.5 Recommends deviations to appropriate DOE directives to S-2.

6.2 Classified Document Custodians (CDCs) and Classified Part Custodians (CPCs) Every organization that possesses classified matter must have one or more Control Stations to oversee the protection of that matter. The number of Control Stations is a management determination. As a minimum, there must be one Control Station for each classified mail stop. At least one primary and one or more alternate CDCs and/or CPCs will staff these Control Stations. These custodians will assist their organizations and fellow employees in the various aspects of classified matter protection and control. Additionally, these primary and alternate custodians will:

6.2.1 Provide S-6 written or electronic notification of their assignment as a custodian within ten (10) workdays of appointment. The notification must indicate group of assignment, classified mail stop, phone number, and whether they are a primary or alternate document or part custodian. S-6 must also be notified within ten (10) workdays when a custodian is replaced.

6.2.2 Receive either “Basic Classified Matter Procedures” training or “Basic Classified Parts Procedures” training from S-6 at the earliest opportunity custodian and training schedules permit. The following courses from DOE’s Central Training Academy may satisfy this requirement:

6.2.2.1 Classified Matter Protection and Control (CMPC) for Custodians (ISC-121D) or

6.2.2.2 Classified Matter Protection and Control (CMPC) I (ISC-221)

6.2.3 Ensure all classified matter generated, received, or transmitted by their organization is properly prepared, marked, and protected in accordance with DOE directives and these procedures.

6.2.4 Ensure all accountable matter within their organization is in an accountability system; all transactions (origination, reproduction, transfer, receipt, destruction, or classification change) are entered into an accountability log; and

all documentation (such as receipts and certificates of destruction) are retained in accordance with General Records Schedule (GRS) 18. When a primary custodian having responsibility for accountable matter is replaced, the outgoing and incoming custodians will conduct an inventory of the accountable matter. Only when all accountable matter has been reconciled will the incoming custodian accept responsibility for the accountable matter. Unresolved differences in the inventory will be reported to S-6 within 24 hours of discovery.

6.2.5 Conduct an annual inventory of all accountable matter in their possession during the fourth quarter of each calendar year.

6.2.6 Conduct or oversee the destruction of accountable and nonaccountable classified matter.

6.3 LANL Use Control Facility Coordinator (UCFC).

6.3.1 Provide, as needed, to the Headquarters Office of Weapons Surety (DP-21) a current roster of all personnel approved for access to Sigma 14 and 15.

6.3.2 Maintain a list of Sigma 14 Weapon Data documents and provide a summary of this information, as requested by the DOE Headquarters Use Control Facility Coordinator.

6.3.3 Serve as point of contact for issues related to Sigma 14 or 15 information.

6.3.4 Coordinate procedures, with appropriate Authorized Derivative Classifiers (ADCs), for identification and categorization of Sigma 14 and 15 information to maintain consistency with the Nuclear Weapons Complex.

6.3.5 Coordinate LANL plans with the appropriate field offices and the DOE Headquarters UCFC.

6.3.6 Ensure LANL compliance with procedures connected to the protection and control of "use control" (Sigma 14 and 15) information.

6.3.7 Ensure personnel authorized access to Sigma 14 or 15 Weapon Data are aware of their responsibilities for the protection and control of this information.

6.4 Users, Owners, or Originators of Classified Matter. All LANL employees and its contractors are responsible for properly protecting classified matter. Additionally, they are to:

6.4.1 Obtain a classification determination from an ADC whenever there is reason to believe any matter may be classified. Additionally, obtain a classification review within 30 days of the creation of classified matter not considered to be an interim product (working papers or drafts, etc.).

6.4.2 Report to the proper classified matter custodian any accountable matter that may not be in an accountability system.

6.4.3 Limit the dissemination of classified matter to those individuals possessing a proper clearance and "need-to-know." An expanded explanation of "need-to-know" can be found at URL: http://www.lanl.gov/fss/fss-15/htmls/restricted/policy_memos.html

6.4.4 Minimize the reproduction of classified matter to that which is necessary for the job to be done.

6.4.5 Protect classified matter against unauthorized disclosure.

6.4.6 Immediately report any known/potential loss or compromise of classified matter to S-6 at 665-1802, but no later than 24 hours after discovery.

6.4.7 Authorize the transmittal of classified matter consistent with the intended recipient's clearance, "need-to-know," and ensure the intended recipient has an approved classified mail address prior to transmittal.

6.4.8 Periodically review nonrecord copies of classified holdings for destruction or refer to S-7 for declassification reviews.

6.4.9 Return classified matter to the proper storage repository when no longer in use.

7 Requirements. DOE M 471.2-1A identifies complex-wide procedures for the protection and control of classified matter. LANL's site-wide requirements are identified below. Additional DOE guidance for the protection and control of classified matter can be found in DOE G 471.2-1A.

7.1 Protection Control and Planning

7.1.1 Deviations. All requests for deviations to the procedures contained herein or to DOE M 471.2-1A will be forwarded to S-6 at mail stop G733. Deviations will be fully justified.

7.1.2 Tier II Self-assessment. S-6 will conduct Tier II self-assessments, not to exceed 18 month intervals, of Laboratory organizations possessing classified matter. Any noted "Observations" will be fixed by the organization with corrective actions forwarded to S-6 no later than two (2) calendar weeks from the completion date of the self-assessment. Any noted "Issues" will require a corrective action plan be sent to S-6, mail stop G733, within four weeks from the final date of the report. The Corrective Action Plan will identify milestones that will be tracked by the organization concerned and S-6 until the "Issue(s)" are closed.

7.1.3 Work for Others (WFO). WFO is work performed by DOE and its contractors for other government agencies, such as the Department of Defense or the Central Intelligence Agency. These projects may be funded partially or entirely by the other federal agencies. When the DOE accepts a WFO project, it also accepts responsibility for following the other agency's regulations, in addition to DOE policies, regarding project-related classified matter.

7.2 Classified Matter In Use/Storage. All classified matter must be stored in accordance with DOE directives. Classified discussions can take place only in approved Security Areas. Hosts of classified meetings, conferences, and discussions are responsible for ensuring those personnel in attendance possess the appropriate clearance level and "need-to-know" for the information being discussed. Hosts are also charged with ensuring attendees do not introduce prohibited articles into the area of discussion, and if necessary, take appropriate measures to ensure aural and visual access is limited only to approved attendees.

7.2.1 In Use Policy for Classified Matter. Based on current DOE provisions and your operational needs, the procedures below establish the circumstances at Los Alamos National Laboratory under which Confidential and/or Secret matter (Restricted Data, Formerly Restricted Data, and National Security Information) may be left temporarily unattended. *These procedures, however, exclude all Top Secret matter, Special Access Program (SAP) matter, Sensitive Use Control Information (SUCI [Sigmas 14/15]) matter, and Special Nuclear Material (SNM)*. Additionally, these procedures do not apply to security areas already approved for open storage of classified matter (e.g., vaults and vault-type rooms).

7.2.1.1 Confidential and/or Secret matter *cannot be left unattended for more than 2 hours*. Ideally, the period of time in which the classified matter is left unattended is kept as short as operationally possible.

7.2.1.2 The classified matter to be left temporarily unattended *must be within a locked room*. All windows must be secured and the room door lock fitted with an approved administrative core and accountable key. (Questions concerning administrative cores and keys should be addressed to S-2 at 5-3433.) Room and door windows must be fitted with blinds, curtains, or other opaque materials to preclude viewing or discovering the room contains classified matter.

7.2.1.3 The lockable room must be located within an *attended security area* (Limited Area, Protected Area, or Exclusion Area). One or more appropriately cleared personnel must be continually present within the security area whenever classified matter is left temporarily unattended in a locked room.

7.2.1.4 Access to classified matter, and subsequent access to locked rooms that may contain unattended classified matter, *must be limited to those with the appropriate security clearance and "need-to-know*."

7.2.1.5 If the highest classification of matter used within an organization is Secret/Formerly Restricted Data, both L- and Q-cleared persons may share a common room key, providing they all share the same "need-to-know."

7.2.1.6 If the highest classification of matter used within an organization is Secret/Restricted Data (or above), only Q-cleared persons may share a common room key--providing they all share the same "need-to-know."

7.2.1.7 *Classified matter must not be left unattended within a locked room or left out within a security area prior to any "announced" fire alarm or similar evacuation-type drill*. All classified matter must be properly secured prior to or at initiation of these tests. Classified matter that is out in a security area or left temporarily unattended in a locked room should not be secured during an "unannounced" or actual life-threatening situation. Depart the area as quickly and safely as possible. In situations where an individual is unsure of the nature of the alarm, assume the worst and immediately evacuate without securing any classified matter.

7.2.1.8 Classified matter may be left temporarily unattended in a locked room *only during normal working hours*, determined by the regular schedule of the security area/organization concerned. Classified matter will never be left temporarily unattended in a locked room either before or after normal working hours.

7.2.1.9 The classified matter left temporarily unattended *must contain all proper classification markings*. Further, the matter must be topped with a classified cover sheet (SF 704 or SF 705) which must be immediately visible upon entering the room. If the classified matter is so large that it cannot be protected by its cover sheet, the matter must be folded, rolled, or covered with opaque material. The cover sheet must then be placed on top so as to be immediately visible when entering the room. (To preclude forgetting that you have unattended classified matter, it *should not* be hidden within the locked room.)

7.2.2 In Use Policy for Vaults/Vault-Type Rooms. Based on current DOE provisions and your operational needs, the procedures below establish the circumstances at Los Alamos National Laboratory under which vaults and vault-type rooms (containing Confidential and/or Secret matter [Restricted Data, Formerly Restricted Data, and National Security Information]) may be left temporarily unattended (defined as locked but not alarmed). *These procedures, however, exclude vaults and vault-type rooms containing Top Secret matter, Sensitive Compartmented Information (SCI) matter, Special*

Access Program (SAP) matter, Sensitive Use Control Information (SUCI [Sigmas 14/15]) matter, computer systems designed to process classified matter, and Special Nuclear Material (SNM).

7.2.2.1 The vault or vault-type room must be located within an *attended security area* (Limited Area, Protected Area, or Exclusion Area). One or more appropriately cleared personnel must be continually present within the security area whenever the vault or vault-type room is left temporarily unattended (locked but not alarmed).

7.2.2.2 The time period in which vaults and vault-type rooms are left locked but not alarmed *should not exceed 2 hours*. Ideally, the period of time in which the vault or vault-type room is left locked but not alarmed is kept as short as operationally possible.

7.2.2.3 Access to the vault or vault-type room combination *must be limited to as few people as possible and only those with the appropriate security clearance and need-to-know*.

7.2.2.4 If the highest classification of matter stored within a vault or vault-type room is Secret/Formerly Restricted Data, a limited number of L- or Q-cleared persons may share the combination, *providing they all share the same need-to-know*. If the highest classification of matter stored within a vault or vault-type room is Secret/Restricted Data (or above), only Q-cleared persons may share the combination, *providing they all share the same need-to-know*.

7.2.2.5 Vaults and vault-type rooms can only be left temporarily unattended (locked but not alarmed) *during normal working hours,* determined by the regular schedule of the security area/organization concerned. Vaults and vault-type rooms must be properly locked (and alarmed) during other than normal working hours.

7.2.2.6 Classified matter left temporarily unattended within a vault or vault-type room *must contain all proper classification markings*.

7.2.3 Form SF 700, Security Container Information. The SF 700 provides the names, addresses, and telephone numbers of employees to be contacted if the security container to which the form pertains is found open and unattended.

7.2.3.1 An SF-700 will be used on each security container, vault, or vault-type room used to store classified matter. (See DOE G 471.2-1A for marking requirements.)

7.2.3.2 Organizations will specify the location for the secure storage of their completed SF-700s.

7.2.3.3 Combinations may only be changed (or set) by personnel with the appropriate security clearance. The Lock Shop (667-4911) must be contacted when combinations require changing. Combinations will be changed for each security container, vault or vault-type room when:

7.2.3.3.1 A new container, vault or vault-type room is put into service.

7.2.3.3.2 Individuals knowing the combination are terminated, transferred, or reassigned.

7.2.3.3.3 Access authorizations for those individuals having knowledge of the combination(s) are downgraded below the level and category of classified matter stored or whose access authorization is administratively terminated, suspended, or revoked.

7.2.3.3.4 A compromise or suspected compromise of a security container, vault or vault-type room or its combination. This includes, but is not limited to, the discovery of a security container, vault or vault-type room left unlocked and unattended.

7.2.3.3.5 A container is taken out of service. The combination will be set to the original factory setting of 25-50-25.

7.2.3.3.6 Combination numbers will be selected at random, avoiding simple ascending or descending series such as 10-20-30 or 50-40-30. Avoid selecting combination numbers that are easily associated with the person(s) selected the combination (e.g., birthdays, anniversaries, social security numbers, or telephone extensions.)

7.2.3.3.7 Prior to moving any security container, complete and forward to S-2 (mail stop G728/665-3433) Form 1657, Security Container Relocation, available at URL: http://enterprise.lanl.gov/forms/1657.pdf

7.2.4 Form SF 701, Security Activity Checklist. The SF 701 provides a systematic means for personnel to make thorough end-of-day security inspections for classified work and storage areas. It also allows for employee accountability in the event that irregularities are discovered. Use of the SF 701 is optional. If used, it should be retained for 3 months from the date of the last entry. The form is available online. Go to URL: http://enterprise.lanl.gov/forms/1691.pdf and select "Activity Security Checklist (1691)

7.2.5 Form SF 702, Security Container Check Sheet. The SF 702 provides a record of the names of persons who have opened, closed, or checked a particular security container holding classified matter. The form also provides a record of the times when those actions were taken. The SF 702 will be retained for 3 months from the date of last entry. The SF 702 is available online. Look for form "1692 - Security Container Check Sheet" at URL: http://enterprise.lanl.gov/forms/1692.pd

7.2.5.1 SF 702s may be placed at the entrance to a room or office containing one or more security containers. Alternate locations include on the outside each safe, vault, or vault-type room. A SF 702 is required for each security container.

7.2.5.2 The form will be annotated to reflect each time the security container, vault or vault-type room is opened and closed. Retain for three months after completion then discard.

7.2.6 End-of-day checks. End-of-day checks are required for each security container, vault or vault-type room used to store/secure classified matter, even if not opened. Exceptions are noted below:

7.2.6.1 End-of-day checks are not required on weekends, holidays, or other non-Laboratory workdays unless the security container, vault or vault-type room was accessed that day.

7.2.6.2 End-of-day checks are not required for security containers, vaults or vault-type rooms where only one individual has the combination and this individual is either on travel, leave, or is sick and the container has not been opened.

7.3 Marking Classified Matter. For additional guidance on marking classified matter, refer to "Checklist for DOE Classification Markings (1/5/95)" at URL: http://www.lanl.gov/fss/fss-15/htmls/restricted/policy_memos.html

7.3.1 Classification Reviews. Classification reviews can only be conducted by an ADC. However, document originators may temporarily assign a classification level and category to matter they believe to be classified. When this process is exercised, a document originator is responsible for obtaining a classification review and determination within 30 days of document origination.

7.3.2 All New Classified National Security Information. Only classified National Security Information created on or after April 1, 1997, will be portioned marked in accordance with DOE directives. A DOE portion marking guide is available at URL: http://www.hr.lanl.gov/SCourses/All/PortionMarking/page01.asp

7.3.3 Mixed Levels and Categories Marking. Organizations must obtain S-6 and S-7 approval prior to using the "Mixed Levels and Categories" marking specified in DOE M 471.2-1A.

7.3.4 Required Classifier Information.

7.3.4.1 For derivatively classified NSI:

Classifier: (Name and Title)
Derived From: (Guide or Source Document and Date)
Declassify On: (Date, Event or Exemption Category)

7.3.4.2 For derivatively classified RD and FRD matter:

Classifier: (Name and Title)
Derived From: (Guide or Source Document and Date)

7.3.5 Distribution of Classified Page Changes

7.3.5.1 The original document distribution list for nonaccountable matter should be used in determining who should receive classified page changes.

7.3.5.2 An accountability log for accountable matter should be used in determining who should receive classified page changes. The accountability log will also reflect the date of destruction for obsolete pages.

7.3.6 Letters of Transmittal (LOT). LOTs accompanying classified NSI-only information need not contain the statement:

"Document transmitted herewith contains: National Security Information."

7.3.7 Working Papers and Drafts. For additional procedures on working papers and drafts, refer to "1690 - Modification Sheet for Classified Working Papers/Drafts" at URL: http://enterprise.lanl.gov/forms/1690.pdf

7.3.7.1 Originators will assign the highest classification level (and category, if RD or FRD) their working papers are anticipated to contain.

7.3.7.2 Originators need not obtain an ADC review if they are knowledgeable of the classification of their material. If they are not, an ADC review is required within 30 days of working paper/draft origination.

7.3.7.3 An ADC review is required within 30 days:

7.3.7.3.1 Of the working paper/draft being formalized into a finished document.

7.3.7.3.2 Prior to sending any working paper/draft outside the Los Alamos National Laboratory complex.

7.3.7.4 Working papers/drafts containing accountable information will require a Unique Identification Number if sent outside the Los Alamos National Laboratory complex.

7.3.7.5 Originators who will be retaining their working papers/drafts beyond 180 days will use form "1690 - Modification Sheet for Classified Working Papers/Drafts" available at URL: http://enterprise.lanl.gov/forms/1690.pdf

7.3.7.6 Working papers/drafts require the markings of a finished document of the same classification when:

7.3.7.6.1 Sent outside the Los Alamos National Laboratory Complex.

7.3.7.6.2 Retained beyond 180 days without modification.

7.3.7.6.3 Filed permanently.

7.3.8 Cover Sheets

7.3.8.1 Locally designed cover sheets will be used for accountable matter while both inside and outside of a security container.

7.3.8.1.1 Form ST-5475 will be used for accountable Confidential matter.

7.3.8.1.2 Form ST-5476 will be used for accountable Secret matter.

7.3.8.2 Cover sheets will not be used as a means for granting access. The possessors of classified documents must ensure they are aware of the contents of the documents prior to release, the purpose being to ensure the intended recipient has the appropriate clearance level and need-to-know.

7.3.9 Protection and Control of Foreign Government Information (FGI). LANL will follow the FGI marking and protection standards identified in DOE M 471.2-1A and DOE G 471.2-1A.

7.4 Accountability and Control Systems. Effective April 1993, LANL implemented DOE's modified accountability program for classified matter, eliminating a number of requirements for much of the Laboratory's classified matter. Classified matter affected by the change now is defined as "nonaccountable." For nonaccountable matter, the following activities are no longer required: maintaining accountability records, conducting and maintaining inventories, certifying destruction, obtaining written authorization to reproduce, and maintaining internal receipting. Although many of the Laboratory's classified documents are nonaccountable under modified accountability, this should not reduce concern for the control and protection of classified matter. Instead, holders of classified matter must now take more individual responsibility for classified matter protection and control.

7.4.1 Detailed accountability records must be maintained on all accountable matter. The following types of classified matter are accountable:

7.4.1.1 Designated Secret and Confidential United Kingdom (UK) "Atomic" matter. (For additional information, refer to "JAIEG - 4, Handbook on Administrative Procedures" for the accountability and Control of United Kingdom Atomic Information. (See Attachment A)

7.4.1.2 Designated Secret and Confidential Foreign Government Information (FGI).

7.4.1.3 Designated Secret and Confidential North Atlantic Treaty Organization (NATO) "Atomal" matter.

7.4.1.4 Sigma 14 matter.

7.4.2 Control Station personnel are referred to as Classified Document or Part Custodians (CDCs or CPCs). These custodians must be designated by their respective organization.

7.4.2.1 BUS-4 is the Central Control Station for all Laboratory incoming and outgoing classified mail and overnight shipments.

7.4.2.2 CIC-14 is the central Control Station for all incoming or outgoing accountable NATO matter. CIC-14 will designate one primary and one or more alternate NATO Control Officers who will oversee the control of such classified matter.

7.4.2.3 CIC-4 is the central Control Station for all designated CRYPTO and COMSEC matter. CIC-4 will designate one primary and one or more alternate control officers who will oversee the control of such classified matter**.**

7.4.3 Each custodian possessing accountable matter will maintain an accountability log. Accountable matter transferred to staff members within the same group will be reflected in the appropriate custodian's accountability log under "Disposition." The staff member will initial the "Disposition" column accepting custody of the matter. The staff member is now responsible for the matter and must notify the appropriate custodian any time the status (transfer, reproduction, destruction, etc.) of the accountable matter changes. Transfer of any accountable matter outside of group channels requires completion of a classified document receipt and annotation of appropriate accountability logs.

7.4.4 Accountability logs will contain the 10 fields of information specified by the DOE. It is understood that our "Authority for Contractor Retention" is DOE Contract W 7405 ENG 36. As a result, this field is need only be listed once in the accountability log.

7.4.5 Accountable matter identified in paragraph 7.4.1 above will be inventoried during the fourth quarter of each calendar year and when there is a change of custodians for accountable matter. S-6 will initiate the Lab-wide inventory. During this annual inventory, the primary custodian will ensure all accountable

matter is in an accountability system, visually verify all accountable matter, and report unresolved discrepancies to S-6 within 24 hours of discovery.

7.4.5.1 Designated Sigma 14 and 15 matter will be controlled, protected, and inventoried in accordance with LANL's "Protection and Control of Sigma 14 and 15 Weapon Data Security Plan." (See Attachment B)

7.4.5.2 Designated CRYPTO and COMSEC matter will be inventoried in accordance with DOE HQ requirements. CIC-4 is the lead organization responsible for the frequency, conduct, and reporting of this inventory.

7.5 Reproduction. Under the provisions of modified accountability, nonaccountable matter may be reproduced without approval. An originator wishing to prevent unlimited copying of classified matter must place the following statement on the first page:

This document may not be reproduced without the consent of the originator, his or her successor, or higher authority.

7.5.1 Authorization. Unless specifically prohibited via a non-reproduction marking caveat, most classified matter may be reproduced without authorization of the originating agency. Reproduced accountable matter requires specific, individual documentation in the appropriate accountability log. This includes a different unique identification number for each copy made.

7.5.2 Matter from Other Agencies. Generally, classified matter sent from other agencies may be reproduced without permission unless the addressee is advised in writing that reproductions require the written consent of the originator.

7.5.3 Top Secret Matter. When noted on the document, written permission from the originator may be required.

7.5.4 Copy Machines

7.5.4.1 Copying of classified matter can only be done by individuals with the appropriate security clearance and "need-to-know." Additionally, copy machines will be inspected by S-5 (Technical Security Countermeasures team) prior to placing them in service.

7.5.4.2 Location. Any machine used for reproduction of classified matter must be located within a security area.

7.5.4.3 Access. Classified copying must not be performed in the presence of uncleared persons or persons without the proper clearance level.

7.5.4.4 Posting. Notices specifying the restrictions and requirements for reproducing classified matter must be conspicuously posted next to the equipment.

7.5.4.5 Clearing. Persons reproducing classified matter on a copy machine must make certain that no classified waste is trapped or left in the equipment and must clear all possible residual classified images.

7.6 Receipt and Transmission of Classified Matter

7.6.1 Control Stations. Control Stations are staffed by trained Classified Document and Part Custodians who oversee the receipt and transmission of classified matter. Contact BUS-4 (Dolores Martinez at 665-4333, pager# 104-3666, or cell phone# 699-0664) for the pick up and delivery of all classified mail. Classified shipments and FedEx deliveries must be coordinated through the BUS-4 shipping office at 667-0996. Unclassified mail/shipments off-site must not be sent through classified mail channels.

7.6.1.1 Inspection of Incoming Classified Mail. Control Station personnel will examine all incoming classified mail for evidence of tampering, improper packaging, and incorrect addressing. Problems will be immediately reported to S-6. Care will be taken to preserve any evidence until delivered to S-6.

7.6.1.2 Classified Mail Preparation. Control Station personnel will ensure classified matter being hand carried or mailed is properly prepared. This includes ensuring the intended recipient has an approved classified mailing address, proper wrapping of classified matter, and preparation of receipts, as required. Control Station personnel (or the Technical Staff Member) must ensure the intended recipient has the proper security clearance and need-to-know for the matter being transmitted.

7.6.1.3 Tracing Lost Shipments. Control Station personnel will initiate tracer actions for all receipts not returned within 30 days for all accountable and Secret matter mailed outside the Laboratory complex, or 14 days for all accountable matter mailed inside the Laboratory complex, which includes the LAAO site.

7.6.2 Classified United States Postal Service (USPS) Mailing. Addresses must be verified through the Laboratory's All-in-One Mailing System or by contacting either CIC-10 (Joe Duran at 665-4567) or S-6 (Mary Ann Lujan at 665-1802).

7.6.2.1 Classified USPS Mailing Address. The Laboratory's classified USPS mailing address is:

7.6.2.1.1 Outer Envelope:

Los Alamos National Laboratory
Attn: Mail Station 5000
For: (Group, Classified Mail Stop)
PO Box 1663
Los Alamos, NM 87545

7.6.2.1.2 Inner Envelope:

Los Alamos National Laboratory
Attn: Mail Station 5000
For: (Recipient, Group, Classified Mail Stop)
PO Box 1663
Los Alamos, NM 87545

7.6.2.2 Classified USPS Return Address. The Laboratory's classified USPS mailing return address is:

7.6.2.2.1 Outer Envelope:

Los Alamos National Laboratory
Attn: Mail Station 5000
From: (Group, Classified Mail Stop)
PO Box 1663
Los Alamos, NM 87545

7.6.2.2.2 Inner Envelope:

Los Alamos National Laboratory
Attn: Mail Station 5000
From: (Recipient, Group, Classified Mail Stop)
PO Box 1663
Los Alamos, NM 87545

7.6.3 Classified Federal Express (FedEx) Shipments. The authorization to use Federal Express has been added to other DOE-approved methods of classified matter transmittal. (At the present time, FedEx is not approved for the transmittal of Top Secret matter.)

7.6.3.1 Permitted Classification Levels. Federal Express can only be used for the transmission of Secret and/or Confidential matter (documents or materials) within the continental United States when determined to be the most cost effective way to meet program requirements.

7.6.3.2 Direct Delivery. To ensure direct delivery to the addressee, the release signature block #7 on the Federal Express Airbill Label must not be executed under any circumstances.

7.6.3.3 Contents Identification. The documents or material being shipped must not be identified as classified matter to Federal Express employees or by marking the outer wrapper as classified.

7.6.3.4 Dispatch. The properly wrapped package must be hand carried to the BUS-4 shipping office by 1:00 p.m. This will allow sufficient time for dispatch on the same day and ensure BUS-4 will not have to secure your classified package overnight.

7.6.3.5 Drop Boxes. Classified matter must not be placed in Federal Express drop boxes.

7.6.3.6 Size and Weight. Classified shipments must meet Federal Express size and weight limitations. However, they offer overnight freight service for large, bulky, or extremely heavy items. These shipments must be coordinated through the BUS-4 shipping office at 667-0996.

7.6.3.7 Weekends and Holidays. Federal Express is not approved for storage of classified matter. Therefore, this service shall not be used on Fridays or on the day proceeding a holiday unless prior assurance has been received the intended recipient (or other appropriately cleared individual) will be available to receive the shipment upon arrival.

7.6.3.8 Prior Notice to Recipient. The sender must inform the intended recipient of the shipment before mailing. The recipient shall be provided the Airbill number for tracking purposes. All packages can be tracked 24 hours a day. This can be done over the telephone by calling 800-238-5355, on the Internet at URL: http://www.fedex.com or through free Federal Express "tracking software."

7.6.3.9 Incoming Shipments. The intended recipient should notify BUS-4 (John Maestas at 7-4186) of any known incoming FedEx classified documents or materials and provide all Airbill numbers. LANL-wide delivery by BUS-4 can only be made to appropriate custodians or recipients at classified mail stops. Classified packages that cannot be picked up or delivered by the end of the day will be temporarily stored in the BUS-4 classified vault.

7.6.3.10 Reporting Problems. Any problems encountered using Federal Express, for the transmission of Secret and/or Confidential matter, are to be reported to either the BUS-4 shipping office at 667-0996 or S-6 at 665-1802.

7.6.3.11 Packaging. DOE procedures concerning double wrapping, addressing and receipting remain in effect, except documents must be double wrapped before placing inside a Federal Express envelope.

7.6.3.12 Addressing. Addresses using a Post Office box are not permitted. The provisions for properly addressing classified matter must be followed. Therefore, classified matter shall be addressed only to *Overnight/Classified Common Carrier Addresses* listed in the DOE Safeguards and Security Information Management System. These addresses are available online from CIC-10's All-In-One-Mail system. If you do not have online access, call 665-4567. CIC-10 will provide instructions for obtaining online access or provide the requested address(es) for you. Alternative methods include contacting the recipient's security office, a DOE security office, or S-6 (665-1802).

7.6.3.13 Classified Federal Express Mailing Address. The Laboratory's classified shipping/FedEx address is:

7.6.3.13.1 Outer Package

Los Alamos National Laboratory
Attn.: John Maestas
For: (Group, Classified Mail Stop)
Building SM-30, Bikini Atoll Road
Los Alamos, NM 87545

7.6.3.13.2 Inner Package

Los Alamos National Laboratory
Attn: John Maestas
For: (Recipient, Group, Classified Mail Stop)
Building SM-30, Bikini Atoll Road
Los Alamos, NM 87545

7.6.3.14 Classified Federal Express Return Address. The Laboratory's classified return shipping/FedEx address is:

7.6.3.14.1 Outer Package

Los Alamos National Laboratory
Attn: John Maestas
From: (Group, Classified Mail Stop)
Building SM-30, Bikini Atoll Road
Los Alamos, NM 87545

7.6.3.14.2 Inner Package

Los Alamos National Laboratory
Attn: John Maestas
From: (Recipient, Group, Classified Mail Stop)
Building SM-30, Bikini Atoll Road
Los Alamos, NM 87545

7.6.4 Hand Carrying Classified Matter within LANL. The following procedures apply to employees hand carrying classified matter within or between Laboratory security areas (including hand carrying to the LAAO site). These procedures, however, do not apply to site delivery personnel. (BUS-4 will develop their own delivery procedures and coordinate them with S-6.) Further, classified matter may only be hand carried while in the performance of official Laboratory duties. Those transporting classified matter must possess the appropriate security access authorization, need-to-know, and programmatic or special access approval for the matter being hand carried. Classified matter shall be prepared in a manner that ensures adequate security protection for the classification involved, the method of transport, and the route of travel. Double wrapping is not required; however, in all cases, measures shall be taken to protect against unauthorized disclosure during transport. As a minimum:

7.6.4.1 Within Security Areas. Top Secret matter will contain a cover sheet (SF 703) and will be placed within a sealed opaque envelope. (The gummed envelope flap must be moistened and sealed; taping the

sealed flap or other seams are optional. If the opaque envelope does not have a gummed flap, but instead uses a metal clasp or string, taping the loose flap is required.) Secret or Confidential matter requires only the appropriate cover sheet (SF 704 or SF 705) to protect the contents from view. If the matter is so large that a cover sheet alone cannot protect the exposed information, then the matter must be folded, rolled, or enclosed within opaque material. The most direct route of travel should be taken minimizing intervening stopover points.

7.6.4.2 Between Security Areas. All classified matter hand carried outside of a security area will have an appropriate cover sheet and be placed within a sealed opaque envelope. (The gummed envelope flap must be moistened and sealed--taping the sealed flap or other seams are optional. If the opaque envelope does not have a gummed flap, but instead uses a metal clasp or string, taping the loose flap is required.) The opaque envelope will be appropriately marked with the name, organization, and classified mail stop of both the sender and recipient. To avoid bringing attention to the document, a classified cover sheet or other classification markings will not be placed on the outside of the opaque envelope. A locked briefcase may serve as the opaque envelope when classified matter is being hand carried. However, the briefcase must have an attached identification tag with the name, organization, and classified mail stop of the hand carrier. If the briefcase is to be opened in transit and while outside of a security area, the classified matter shall be placed within a sealed (or taped) opaque envelope. The most direct route of travel should be taken minimizing intervening stopover points.

7.6.4.3 Receipts

7.6.4.3.1 Receipts are not required for hand carrying classified nonaccountable matter within the Laboratory complex (to include hand carrying classified nonaccountable matter to LAAO).

7.6.4.3.2 DOE F 5635.3, "Classified Document Receipt," or the Laboratory's "Classified Document Receipt," ST 4189 or ST 5483, shall be used when hand carrying accountable matter. For accountable matter, the transferring custodian will retain a suspense copy of the receipt until the hand carrier returns the signed receipt.

7.6.4.3.3 If the hand carrier does not return the receipt (for accountable matter) to the original custodian, a suspense date (not to exceed 14 days for internal hand carry or 30 days for external hand carry) shall be established. Follow-up or tracer action must be initiated if the signed receipt is not returned within the appropriate suspense period.

7.6.5 Hand Carrying Classified Matter Off the Hill. It is no longer a requirement to authorize, in writing, persons hand carrying classified matter within the United States. However, appropriate LANL management must approve all classified matter hand carried off-site. Additionally, individuals hand carrying classified matter off the Laboratory must comply with the following requirements:

7.6.5.1 Travelers hand carrying classified matter must be appropriately briefed as to their security responsibilities. This can be accomplished be reading and signing the "Briefing to Hand Carry Classified Matter (1658)" found at URL: http://enterprise.lanl.gov/forms/1658.pdf

7.6.5.2 This form must be read and signed annually for those who hand carry classified matter to locations throughout the United States. Those whose job would not entail this responsibility need not complete this form.

7.6.6 Hand Carrying Classified Matter on Airplanes

7.6.6.1 Matter Which Can Be X-Rayed. Travelers hand carrying classified matter in the form of paper documents, vu-graph material, film products, computer media, etc., are able to pass their matter through airport X-ray equipment without concern of compromising their information. (This assumes the traveler has placed nothing else in the package, which would arouse suspicion on the part of airport security officials.) In these situations, a Letter of Authorization is not required. For those staff members who would like the assurance of exempting airport security officials from examining their classified matter, a sample "Letter of Authorization to Exempt Physical Examination(1655-a)" can be found at URL: http://enterprise.lanl.gov/forms/1655.pdf

7.6.6.2 Matter Which Cannot Be X-Rayed. Employees hand carrying classified matter which would be compromised by X-ray examination are required to carry a Letter of Authorization during travel. This includes, for example, metal parts whose shape is classified. Please note that material, which can be X-rayed without compromising its information, cannot be exempted from x-ray examination. Exempting any material from X-ray examination requires prior coordination with the airline of initial debarkation--not airport security officials. Then upon check-in, present the airline with an original Letter of Authorization. After they check your identification, they will escort your classified material through security. A sample "Letter of Authorization to Exempt X-ray Examination(1655)" can be found at URL: http://enterprise.lanl.gov/forms/1655.pdf

7.6.7 Transmission of Classified Matter to a Foreign Government. Laboratory personnel having a need to transmit classified matter to a foreign government or an international organization will submit a written request to S-6, identifying the information for disclosure, reason for disclosure, and the anticipated date and location of disclosure. Until a final release authorization is received from the Department of Energy, the information in question may not be released under any circumstances. The same procedures apply if hand carrying classified matter outside of the continental limits of the United States.

7.6.8 Electronic Transmission of Classified Matter. When any classified matter is transmitted electronically, the method selected must be approved for the classification level and category of information transmitted. The method selected also must have an approved security plan and procedures to process the information appropriately.

7.7 Protection and Control of Sigma 14 and 15 Weapon Data. See LANL's "Protection and Control of Sigma 14 and 15 Weapon Data Security Plan." (Attachment 2)

7.8 Assignment of Sigma Authorities

7.8.1 When access to Sigma 1 is authorized, access to Sigmas 1 - 10 is approved.

7.8.2 When access to Sigma 2 is authorized, access to Sigmas 2 - 10 are approved. Do not allow access to Sigma 1 data.

7.8.3 When access to Sigma 3 is authorized, access to Sigmas 3 - 10 are approved. Do not allow access to Sigmas 1 and 2 data.

7.8.4 When access to Sigmas 4–11 are authorized, access is limited only to the individual Sigma authorized and does not extend to other Sigmas.

7.8.5 When access to Sigma 12 is authorized, access to Sigma 13 is also approved. Authorization for Sigma 13 only does not include access to Sigma 12.

7.8.6 When access to Sigma 14 is authorized, access to Sigmas 1–11 and 15 are also approved. Authorization for Sigma 14 does not include assess to Sigmas 12–13.

7.8.7 When access to Sigma 15 is authorized, access to Sigmas 1–11 is also approved. Authorization for Sigma 15 does not include assess to Sigmas 12–14.

7.9 Contract Close-out/Facility Termination. The S-6 FOCI/FDAR Program Manager (665-1624) will work with the appropriate contractor Facility Security Officer (FSO) whenever a LANL contract involving access to classified matter or unescorted entry into Laboratory security areas is completed or terminated. The FOCI/FDAR Program Manager will:

7.9.1 Initiate documentation to cancel the appropriate facility approval.

7.9.2 Coordinate with the appropriate BUS-5 contract administrator and contractor FSO to ensure all classified matter (accountable and nonaccountable) is returned to the Laboratory, or appropriate retention authorization has been obtained.

7.9.3 Work with the contractor FSO to ensure all DOE access authorizations are terminated and all security badges returned.

7.10 Destruction. For additional information regarding the destruction of sensitive unclassified and classified waste, please refer to "Destruction of Nonrecord Copies of

Sensitive Unclassified and Classified Waste (5/31/95)" at URL:
http://www.lanl.gov:80/orgs/s/s6/infosec/policy_memos.html

7.10.1 Classified holdings must be reviewed periodically with the emphasis on reducing our nonrecord copies of our unclassified and classified holdings. You may need to check with CIC-10 to determine if DOE has placed a moratorium on the destruction of your specific classified information.

7.10.2 Only approved shredders will be used to destroy classified matter. Additionally, JCNNM (667-2109) may be contacted for the destruction of large volumes of classified matter.

7.10.3 The destruction of all accountable matter must be documented, as required. Top Secret destruction records will be retained for five (5) years. Secret and Confidential accountable records will be retained for two (2) years.

7.10.4 Classified matter awaiting destruction must be stored in approved classified repositories.

7.11 Material

7.11.1 Classified parts meeting the accountability definitions of section 7.4.1 above must be brought into an accountability system. In instances where this is not practical due to size, composition, configuration, etc., contact S-6 for additional guidance. No formal accountability is required for nonaccountable parts.

7.11.2 When hand carrying classified parts, care must be taken to prevent unauthorized access. This may mean enclosing the part(s) in an envelope, bag, or box.

7.12 Emergency Procedures. Personal safety is always the Laboratory's top priority. In the event of any perceived or actual life-threatening situation, personnel will immediately evacuate the area of danger.

7.12.1 Personnel should exit the building in an orderly manner. If this is an exercise, the exercise staff and/or PTLA are responsible for building security throughout its conduct.

7.12.2 DOE's two-hour (2-hour) in use policy for unattended classified matter is automatically extended to include the length of any exercise.

7.12.3 Custodians and others who may have left classified matter out as a result of an exercise will conduct a post exercise inventory of the classified matter. Discrepancies will be immediately reported to S-6 at 665-1802.

7.12.4 PTLA is responsible for providing continuous security for the affected areas. A post-emergency recovery and inventory will be conducted only when safe to do so. Any debris determined to be classified will then be properly secured by PTLA or others, as determined.

7.12.5 Circumstances where safety is paramount, access to classified matter must be granted. Access to classified matter can even be provided to uncleared individuals when life-threatening situations occur. However, in life-threatening situations where classified matter is provided to uncleared individuals, S-6 must be notified immediately following such events.

7.13 Unaccounted-for Matter and Compromise of Classified Information. Upon discovering that classified matter is unaccounted for, potentially compromised or compromised, personnel must immediately report the incident to a supervisor and to S-6 at 665-1802.

7.13.1 Unaccounted-for Matter—classified matter that cannot be located.

7.13.2 Potentially Compromised Matter—classified matter that might have been compromised, for example, by being left unattended on top of a desk where unauthorized personnel may gain access to it.

7.13.3 Compromised Matter—classified matter that has been disclosed to unauthorized personnel, for example, by being published in a magazine or newspaper.

7.14 Security Infractions. An infraction is any act or omission that involves failure to comply with DOE or LANL safeguards or security procedures. The following are some, but not all, of the most common security infractions:

7.14.1 Failure to properly secure a security container.

7.14.2 Leaving classified matter improperly secured while in use.

7.14.3 Improperly preparing classified matter for transmittal.

7.14.4 Leaving a computer system unattended while it is processing classified data.

7.14.5 Removing classified matter from a security area without proper authorization.

7.14.6 Improperly destroying classified matter.

7.14.7 Discussing classified information in the presence of or within hearing of unauthorized persons.

7.14.8 Discussing classified information over unsecured telephone systems.

7.14.9 Failing to escort or improperly escorting uncleared persons in security areas.

7.14.10 Failing to obtain proper classification reviews of potentially classified matter.

7.15 Security Infraction Inquiry Procedures. Employees are responsible for reporting violations of security policies and procedures to their supervisors. Supervisors (or employees) must also notify the appropriate LANL security group.

7.15.1 An inquiry into the security incident will be conducted by the appropriate LANL security organization. If an infraction is warranted, a LANL Infraction Report will be prepared and sent to the appropriate Division Director/Program

Manager for action. A response will be prepared and the report returned within 15 calendar days. This response should confirm in writing that the details, as reported, are essentially correct. The individual receiving the security infraction will sign the report.

7.15.2 If management believes that an infraction is not warranted, they must either:

7.15.2.1 Supply evidence to support a finding that the details of the report were incorrect, or

7.15.2.2 Identify mitigating circumstances that should preclude a security infraction from being changed.

7.15.3 Management must also identify corrective action(s) in the LANL Infraction Report that will result in a reduced probability of recurrence.

7.15.4 The original, completed LANL Infraction Report will be forwarded to DOE/LAAO. Trending data will be used to modify safeguards or security procedures and security education programs.

7.16 Security Infraction Disciplinary Actions. Appropriate corrective action must be initiated in all cases where an individual is charged with a security infraction. S Division may recommend appropriate corrective action, including a letter of reprimand, badge confiscation, disciplinary leave or termination. An infraction that requires such adverse corrective action will be coordinated through HR-2-ER. The following schedule describes appropriate disciplinary measures for infractions occurring within any 12-month period, except in cases where consideration is being given to suspension or termination of clearance for serious or repeated security infractions impacting national security.

7.16.1 First Infraction. (See AM 112.14 and AM 112.18)

Oral Counseling: Emphasize the seriousness of the incident and the importance of care and concern for security procedures. The employee should be advised of the consequences for subsequent infractions. The counseling should be conducted by the employee's Group Leader or next higher level of management, if appropriate. Documenting the meeting is appropriate and documentation should be maintained in the employee's organization file.

7.16.2 Second Infraction. (See AM 112.14 and AM 112.19)

Written Counseling: A verbal reprimand will be made by the employee's Division Director or next higher level of management, as appropriate. A memorandum documenting the meeting will be sent from the Division Office to the employee describing the infraction, noting the previous oral counseling effort, and precedures for avoiding further infractions, and the consequences for any subsequent infraction. A copy of the memorandum will be filed in the employee's Group and Division Office files.

7.16.3 Third Infraction. (See AM 112.15 and AM 112.22)

Written Reprimand: The Group Leader, or next higher level of management, if appropriate, will prepare a written reprimand, in consultation with HR-2-ER, that follows the procedures outlined in AM 112.22. The reprimand will be placed in the employee's official Personnel Records for two years.

7.16.4 Adverse Corrective Action. (See AM 112.20)

More than three infractions in one 12-month period, or a serious offense, may justify adverse corrective action. These measures may include a recommendation for disciplinary leave without pay or termination of employment. These actions must be coordinate with HR-2-ER and reviewed by a Case Review Board.

7.16.5 Badge Confiscation. (See AM 112.44 and AM 702.17)

Severe infractions may warrant removal of the employee from his or her work area or the Laboratory. In these cases, the employee's Group Leader may confiscate the employee's security badge, with the concurrence of the HR Director. Usually the employee will be placed on investigatory leave while the situation is assessed.

7.16.6 Clearance Suspension. (See AM 702.21)

DOE may suspend and employee's clearance pending resolution of questions concerning and employee'' continued eligibility to hold a clearance.

8 Documentation. None.

9 References

9.1 DOE Manual 5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests.

9.2 DOE Order 471.2, Information Security Program.

9.3 DOE Manual 471.2-1A, Manual for Classified Matter Protection and Control.

9.4 DOE Guide 471.2-1A, Classified Matter Protection and Control Implementation Guide.

9.5 DOE General records Schedule 18.

10 Attachments

10.1 Attachment A: JAIEG – 4, Handbook on Administrative Procedures for the Accountability and Control of United Kingdom Atomic Information. (Available from group S-6, 665-1802.)

10.2 Attachment B: Protection and Control of Sigma 14 and 15 Weapon Data Security Plan. (URL is: http://www.lanl.gov/internal/security/sigma14_15.html.)